

クラウド型 IT 資産管理システム 一式

(Cloud-based IT asset management
system)

仕 様 書

平成28年6月

独立行政法人 国立高等専門学校機構

目次

目次	- 1 -
I. 仕様概要説明	- 2 -
1. 調達背景及び目的	- 2 -
2. 契約期間	- 2 -
3. 調達物品名及び構成内訳	- 2 -
4. 技術的要件の概要	- 2 -
II. 調達物品に備えるべき技術的要件	- 3 -
5. 性能, 機能に関する要件	- 3 -
5.1. 基本要件	- 3 -
5.2. 機能要件	- 5 -
III. 導入実施と納品に備えるべき要求要件	- 10 -
6. 導入支援作業	- 10 -
6.1. SaaS 型 IT 資産管理システムの利用準備	- 10 -
6.2. 管理対象 PC へのインストール	- 10 -
7. 提案事業者を求める事項	- 10 -
7.1. 製品に関する事項	- 11 -
8. 性能, 機能以外に関する要件	- 10 -
8.1. 受注要件	- 10 -
8.2. 保守要件	- 10 -
8.3. 操作教育・研修	- 11 -
8.4. 機密保持	- 11 -
8.5. 検査及び検収	- 11 -
8.6. 損害賠償	- 12 -
8.7. その他	- 12 -

I. 仕様概要説明

1. 調達背景及び目的

独立行政法人国立高等専門学校機構（以下「機構」という。）において利用しているオンプレミス型 IT 資産管理システムからクラウド型へ移行するにあたり IT 資産管理システムの新規調達及び設定等を目的とする。

2. 契約期間

本調達物品について、下記の契約期間とすること。

契約期間：平成 28 年 1 月 1 日～平成 34 年 1 月 30 日 [6 年間]

3. 調達物品名及び構成内訳

(調達物品名)

クラウド型 IT 資産管理システム 一式

(構成内訳)

- (1) SaaS 環境
- (2) IT 資産管理システム 一式
- (3) 機器への導入・調整・運用支援 一式

4. 技術的要件およびその他の要件の概要

- ① 本調達物品に係る性能、機能及び技術等（以下「性能等」という。）の要求要件（以下「技術的要件」という。）は、「Ⅱ 調達物品に備えるべき技術的要件」に示すとおりである。
- ② ①以外の要求要件（以下、「その他の要件」という。）は、「Ⅲ. 導入実施と納品の備えるべき要求要件」に示すとおりである。
- ③ 技術的要件およびその他の要件はすべて必須の要求要件である。
- ④ 必須の技術的要件およびその他の要件は機構が必要とする最低要件を示しており、入札物品の性能等がこれらを満たしていないとの判定がなされた場合には不合格となり、落札決定の対象から除外する。
- ⑤ 入札物品の性能等が技術的要件を満たしているか否かの判定は、技術審査において、入札物品にかかる技術仕様書その他の入札説明書で求める提案資料の内容を審査して行う。

II. 調達物品に備えるべき技術的要件

5. 性能、機能に関する要件

5.1. 基本要件

(1) 導入構成に関する要件

- ① 機構が所有する管理対象 PC 全 30,000 台について、インベントリ情報収集と IT 資産管理台帳を実現するために必要な IT 資産管理システムを導入する。
- ② 機構が設置する国立高等専門学校 (全 51 校 55 キャンパス), 及び機構拠点内に存在する管理対象 PC を対象とする。
- ③ IT 資産管理システムは, SaaS 型で導入することとし, 管理用のサーバー機器, サーバースステムの導入は, サービスとして利用することとする。また, 必要となるデータベースソフト等のミドルウェア類を含め, これらに要する費用は, 応札業者の負担とし, 調達金額に含めるものとする。
- ④ 各高専や拠点等には, データ中継用サーバー, 管理対象 PC 台数に応じた分散サーバーなどの一切の設備負担をすることなく, 導入が可能であること。
- ⑤ 管理対象 PC からの PC 情報の収集, 及び各種管理台帳及びレポートの利用に際しては, HTTPS 通信で経路暗号化を行うこと。
- ⑥ HTTPS 通信においては, 信頼に足る実績豊富なベンダーの SSL サーバー証明書を必須とし, デジタル署名を付与すること。ただし, アクセス先 URL に機構の指定ドメインを利用可能な場合, SSL サーバー証明書は機構にて用意するものとし, それを受領して設定等を行うこと。

(2) SaaS システム基盤に関する要件

- ① あらゆる災害に備えた堅牢なファシリティと, 厳重なセキュリティ対策が施された, 日本国内にある Tier3 相当以上のデータセンター上に構成されること。
- ② 万一の物理サーバー故障時においても, 5 分以内を目安として, 他の物理サーバーに切り替わり再起動され利用可能であること。
- ③ 資産管理データベース及びシステムは, RAID6 相当以上の構成で冗長化されたディスクに格納すること。
- ④ システム構成コンポーネントは全て二重化し, 高信頼性を確保すること。
- ⑤ DDos 攻撃やウイルス・スパイウェア対策など, 万全のセキュリティ対策が施されていること。
- ⑥ データセンター内への入退室管理について, 24 時間の監視, ID カード等による不正入室の排除, 監視カメラ, ネットワークの監視等を備えること。
- ⑦ 情報セキュリティマネジメントシステム (ISMS) の国際規格「ISO/IEC27001」を取得し, かつ, 米国公認会計士協会の基準に基づき提供される内部統制の仕組み「SOC2 保証報告書」を受領している, 第三者機関の評価としても信頼に足るデータセンターを利用すること。
- ⑧ データセンターのサーバー稼働率は 99.98%以上を SLA として保証すること。
- ⑨ クラウド型 (SaaS 型) IT 資産管理システム (以下「管理システム」という) は, 定期保守等の計画停止を除き, 99%以上の稼働率を SLA として保証すること。
- ⑩ 管理システムは, 財団法人マルチメディア振興センターの運用する「ASP・SaaS 安全・信頼性に係る情報開示認定制度」の認定, もしくは, 特定非営利活動法人

ASP・SaaS・クラウドコンソーシアムの主催する「ASP・SaaS・クラウドアワード」を受けていることとし、第三者機関の評価として信頼に足る SaaS システムであること。

- ⑪ 管理システム上のデータは、適切なバックアップを行い、万一の際に少なくとも前日の状態に戻せるようにすること。

(3) 管理対象 PC に関する要件

- ① 管理対象 PC として以下の全ての OS に対応していること。

Windows	<p>★Windows 10 (Pro, Enterprise, Education, Home)</p> <ul style="list-style-type: none"> ・Windows 8.1 (無印, Pro, Enterprise) ・Windows 8 (無印, Pro, Enterprise) ・Windows 7 (Starter, Home Premium, Professional, Enterprise, Ultimate) ・Windows Vista (Home Basic, Home Premium, Business, Enterprise, Ultimate) ・Windows XP (Home Edition, Professional) ・Windows Server 2012, 2012 R2 ・Windows Server 2008, 2008 R2 ・Windows Server 2003, 2003 R2 <p>※32bit 版と 64bit 版に対応すること</p>
Macintosh	<p>★Mac OS X 10.11</p> <ul style="list-style-type: none"> ・Mac OS X 10.10 ・Mac OS X 10.9 ・Mac OS X 10.8 ・Mac OS X 10.7 ・Mac OS X 10.6

- ② Windows, Mac OS X の新たな OS への対応については、システム保守の一環として契約費用の範囲で提供すること。
- ③ 各 OS の日本語版と英語版に対応すること。
- ④ 仮想 OS 上で運用されている場合や、異なる OS を多重起動している場合も、各 OS 環境での PC 情報を収集する機能を有すること。
- ⑤ 管理対象 PC は、ドメイン未参加など多様な形態で利用されているため、本システム以外に、エージェント（「5.2(2) インベントリ情報収集」を参照）を除く特殊なソフトウェアのインストールや、ポート開放を含むネットワークの設定など、事前に特段の変更をせずに利用可能であること。
- ⑥ 有線 LAN, 無線 LAN などのネットワーク接続形態、また NAT または NATP によって接続されている場合においても、PC 情報を収集する機能を有すること。
- ⑦ 収集した PC 情報を管理システムの管理サーバー（以下「管理サーバー」という）に送信する際には、HTTPS 通信による経路暗号化をすること。また、プロキシ環境を有する場合等についても PC 情報の収集が可能であること。
- ⑧ 管理対象 PC への本システム展開に際しては、管理サーバーにログインしてダウンロード実行することで、利用者自身が簡単な方法で実施できること。

(4) ライセンス形式に関する要件

- ① 年度ごとの管理対象 PC のリプレース等を想定し、契約は年度ごとの利用料金制にて行うものとする。管理対象 PC が入れ替わった際でも、当該年度の終了時点で

契約台数を大幅に超えないことを条件に、この利用料金の中で対応可能であることとし、入替後の新規管理対象 PC に対するライセンスを含むものであること。

- ② 年度ごとの利用料金の中には、全てのシステム保守、システムのバージョンアップの無償権、サポートデスク（問い合わせ窓口）利用料金を含むものとする。
- ③ SaaS 利用環境の準備や設定等については、契約初年度での契約とする。

5.2. 機能要件

(1) 全般及び基本機能

- ① 管理システムが作成する各種管理台帳及びレポートは、機構を最上位とし、各高専・学科・研究室・センターといった管理階層ごとに作成すること。これを「管理単位」と称する。また、「事務系」「教育系」や「教員用」「学生用」といった仮想の階層を設けられること。この階層管理により、機構本部管理者及び高専管理者（以下「各管理者」という）に対して管理範囲に応じた権限設定ができること。なお、管理階層の情報は機構から指示された階層を設定すること。
- ② 管理階層は、最大で 10 階層以上作成可能なこと。また各階層 1 管理単位の直下に作成可能な管理単位は 20 以上であること。
- ③ 各管理者が専用の管理機を用意することなく、業務で通常使用している PC を管理用端末として使用できること。また、各種台帳及びレポートは、全て Web ブラウザからの閲覧・管理が可能であること。アドオンのインストールを含め、何らかの追加対応を行うことなく利用可能であること。
- ④ 各種管理台帳及びレポートは、日本語表示と、英語表示を切り替えて利用可能であること。
- ⑤ 管理対象 PC への本システム展開稼働後も、リソースの消費は最小限に抑えること。利用者が特段の意識をすることなく、通常通り業務が可能であること

(2) インベントリ情報収集

- ① 管理対象 PC のインベントリ情報を収集するプログラム（以下「エージェント」という）の展開においては、利用者が管理サーバーへ Web ブラウザからアクセスしログインすることで実行できる容易な仕組みであること。
- ② エージェントは、初回実行時に、管理対象 PC にインストールされ機構管理者が設定するスケジュールで定期的にインベントリ情報収集が自動実行される常駐タイプと、PC にプログラムファイル等を残さない非常駐タイプを用意し、管理対象 PC や各高専、利用組織の特性や要件に応じて選択可能であることと。
- ③ 常駐タイプのインベントリ情報収集については、定期的な自動実行の他に、管理対象 PC からの利用者による随時起動が可能であること。
- ④ Web ブラウザは、Internet Explorer, FireFox, Safari, Google Chrome に対応し、各 OS 環境からのマルチブラウザアクセスに対応すること。
- ⑤ 定期自動実行によるエージェント起動は、スケジュールされた時刻に集中起動しないよう、実行タイミングをランダムに分散させる負荷分散が図られていること。また、バックグラウンドで行うものとする。
- ⑥ 定期自動実行によるエージェント起動時にネットワークに接続されていない場合や、電源がオフの場合に対し、ネットワーク接続された後、または電源を立ち上げた後に自動的にエージェント起動を実施する機能を有すること。
- ⑦ 定期自動実行によるエージェント起動時に管理サーバーが保守等により停止し

ていた場合でも、管理対象 PC にエラー通知やメッセージを出さないこと。

- ⑧ 収集するインベントリ情報は下記の通り。
- ・ハードウェア情報
「コンピュータ名」、「OS」、「IP アドレス」、「MAC アドレス」、「メーカー名」、「モデル名」、「ハードウェアシリアル番号」、「各種スペック情報 (CPU クロック数、メモリ容量、ハードディスク容量など)」、「ドメイン/ワークグループ情報」
なお「コンピュータ名」や「IP アドレス」は重複が十分予想されるため、PC の識別のキー項目として用いてはならない。これらが重複するような場合でも、固体識別が問題なく可能であること。
 - ・属性情報
「管理単位 (高専名・所属の・学科・研究室や部局組織等)」、「設置場所」、「使用者名」、他 (「物品管理の番号」、「利用用途」、「資産の種別」、「備考」などを想定している)
これら項目については、導入時に機構が指定する内容で収集可能なよう設定をすること。また利用者の負荷軽減のため、項目に応じて、文字入力以外にプルダウン選択等が可能であること。
 - ・ソフトウェア情報
「ソフトウェア名称」、「メーカー名」、「エディション」、「バージョン」、「プロダクト ID」が収集可能であること。
 - ・ウイルス対策状況
シマンテック社・トレンドマイクロ社・マカフィー社・ソフォス社、CA 社、ESET 社のコーポレート版ウイルス対策ソフトウェアについて、「ウイルス対策ソフトウェア名」、「定義ファイルのバージョンと更新日付」、「リアルタイム保護の状態」等の詳細情報を収集できること。
これら以外のウイルス対策ソフトウェアについても、「ウイルス対策ソフトウェア名」は取得すること。
- ⑨ 管理対象 PC の「高専名、専攻科・研究室名」等や「使用者名」、他、機構が指定する管理項目について、入力が可能であり、この内容が各種台帳に反映されること。また負荷軽減のため、入力以外にプルダウン選択なども可能であること。これらはマスターとして導入時にセットアップを行うこと。
- ⑩ ネットワークに接続されないオフライン PC のインベントリ収集にも対応すること。容易に同レベルの情報を収集し、台帳にて管理可能であること。収集したオフライン PC のインベントリ情報は、利用者自身がネットワーク接続 PC から管理サーバーにアクセスし、容易な手順でインポート登録が可能であること。
- ⑪ 教員の PC が高専外に持ち出されて利用されること等を想定し、高専及び機構のネットワーク以外の接続環境 (自宅や長期の海外出張等を含む) においても同様にインベントリ収集可能であること。
- ⑫ CSV 等テキスト形式に、ハードウェア情報、ソフトウェア情報を記入したものをを入力情報としてインポート登録できる機能を備えること。
- ⑬ エージェントのアンインストールに際しては、専用のアンインストーラを用意し、またエージェントを構成するプログラム類はアンインストール後にシステム領域に残存させないこと。

(3) ハードウェア管理台帳

- ① 収集したインベントリ情報から、管理単位ごとに、「ハードウェア管理台帳」を自動的に作成すること。
- ② 管理単位ごとに管理 ID を設定し、自 ID の範囲内での管理、及び上位 ID は下位管理単位の管理を可能とするよう、権限設定が可能であること。また機構管理者

は全高専分の情報を閲覧管理できること。

- ③ 「ハードウェア管理台帳」には、管理単位名、PCの設置場所情報、PCの使用者（もしくは管理者）名、利用の用途などの属性情報と、「コンピュータ名」、「OS」、「メーカー名」、「モデル名」、「IPアドレス」、「MACアドレス」、「各種スペック情報」、「インベントリ情報を取得した日付」を一覧表示させること。
- ④ 台帳画面には各項目を検索条件として用意し、「管理単位」、「設置場所」、「使用者名」、「コンピュータ名」、「OS」、「メーカー名」、「モデル名」等に加え、「属性情報」についても指定しての絞り込み検索が容易に可能であること。
- ⑤ 「ハードウェア台帳」に関する各項目について、全件、また検索絞り込み条件に沿って、容易にCSV形式で出力し、2次利用等が可能であること。
- ⑥ 必要に応じて、「リース管理台帳」、「PC購入台帳」を作成できること。この際、「ハードウェア管理台帳」の情報を活用することで、作成や管理の負担を軽減する措置が講じられていること。

(4) ソフトウェア台帳とソフトウェア資産管理

- ① 収集したインベントリ情報から、全てのソフトウェアの一覧及びインストール数の集計表である「ソフトウェア台帳」、及び管理対象PC別のインストールソフトウェア一覧表となる「PC別ソフトウェア台帳」を自動的に作成すること。
- ② これらソフトウェアの台帳類は、管理単位ごとに作成すること。
- ③ 管理単位ごとに管理IDを設定し、自IDの範囲内での管理、及び上位IDは下位管理単位の管理を可能とするよう権限設定が可能であること。また機構管理者は全部を閲覧管理できること。
- ④ 台帳画面には各項目を検索条件として用意し、「管理単位」、「ソフトウェア名」、「メーカー名」等を指定しての絞り込み検索が容易に可能であること。
- ⑤ 各ソフトウェアはOSプラットフォームを識別し、ソフトウェア台帳類において「Windows版」、「Mac版」等の判別、絞り込み検索等が容易に可能であること。
- ⑥ 管理単位ごとにソフトウェアのインストール数やライセンス数などが集計され、照合確認が可能であること。
- ⑦ ソフトウェアに対し、「管理対象」、「管理対象外」、「未決定」という状態を管理区分として管理できること。同一のソフトウェアでも、管理単位ごとに異なる指定が可能であること。また、Microsoft社やAdobe社の主要製品については、ソフトウェア名称内の詳細バージョン等を識別し、ライセンス管理すべき製品名に名寄せして台帳化すること。
- ⑧ ソフトウェアの主要メーカー名について、管理対象PCから収集した生データのまま台帳にするのではなく、「Adobe社」、「Microsoft社」など、1回の操作で検索可能となるよう、適正なデータ補正を行うこと。
- ⑨ Adobe社のCSシリーズ(Windows版)や、Microsoft社のOfficeシリーズ(Windows版)等について、製品本体と同梱ソフトウェアの識別が可能であり、ライセンスの二重カウント等を防止できること。
- ⑩ インストール数に対して所有のライセンス数の照合を行う「管理対象ソフトウェア」について、「ソフトウェア台帳」上で個別に指定が可能であること。
- ⑪ 機構が独自に設定するソフトウェアのグルーピング情報をマスターとして保持可能であること。機構管理者側での登録・修正・削除が可能であること。ソフトウェア台帳においては、このマスターに「登録済」、「未登録」等の条件を指定して把握することが可能であること。
- ⑫ ライセンス契約情報を登録し、インストール情報と関連付けての内訳の詳細な管理が可能であること。ライセンスによって許諾される、セカンドライセンスやアップグレード・ダウングレードインストールなどの管理が可能であること。管

理単位を横断しての関連付けも可能であること。また、ソフトウェアのグルーピングマスター情報に基づき、ダウングレードの自動判定等が行えること。

- ⑬ アップグレードやダウングレードといった利用に対しては、アップグレードの元となったライセンス情報、アップグレード先のライセンス情報が関連付けて管理され、また利用可能なライセンス数について適正に管理が可能であること。
- ⑭ ライセンス契約情報には、調達したソフトウェアライセンスについての、「ソフトウェア名」、「購入日付」、「購入組織（専攻・学科・組織等）」、「購入理由」、「期間ライセンスの場合の開始日と終了日」、「ライセンス種別」、「数量」、「ライセンス契約形態」、「ライセンス証書番号」、「インストールキー」などの情報を登録できること。この時、「ソフトウェア名」については、収集したインストール名称を指定できるようにして利用者の入力負荷を軽減すること。インストールが行われておらず名称情報が無い場合でも、仮登録を行い、後から再指定等が可能であること。またライセンス契約情報は、画面からの入力による登録以外に、CSV形式のファイルを入力としたインポートによる一括取り込み機能も備えること。
- ⑮ ソフトウェアのグルーピングマスター情報に基づき、所有するライセンス数、関連付けられ消費された数、うちライセンス所有組織と消費組織が異なる数、ダウングレードインストールで消費された数、セカンドライセンス等にて消費された数、これらの合計としての消費数合計、所有するライセンス数との差異を、機構全体、各高専等の管理単位別に集計できること。
- ⑯ 教員が個人で購入したソフトウェアを管理対象 PC にインストールして利用している場合等においても、ライセンス契約情報とインストール実態情報とを紐付け管理することで適切に判別して管理が可能であること。
- ⑰ 棚卸したライセンス証書の現物について、管理台帳データとの連動性を確保するため、管理台帳上に証書原本の有無や資料番号・インデックス（紐付け番号）などの情報を登録でき対応付けて管理できること。
- ⑱ ソフトウェア台帳類に関する各項目について、全件、また検索絞込み条件に沿って、容易に CSV 形式で出力し、2 次利用等が可能であること。この時、ハードウェア及びその属性情報も関連付けて加工利用しやすい形に出力できること。

(5) ソフトウェア辞書と各種ソフトウェア資産管理支援機能

- ① ソフトウェアについて、有償製品、シェアウェア、フリーソフトウェア、ドライバ等、アドウェア・マルウェアといった分類の情報を、ソフトウェア辞書として提供すること。ソフトウェア資産管理台帳にて、管理対象ソフトウェアの選定や、ソフトウェアのグルーピングマスターの設定の際に利用できること。
- ② 分類情報は参考情報とし利用するものとし、機構が独自に判断して分類情報の確定ができるものであること。
- ③ ソフトウェアの分類情報については、機構が調査して判明した情報などを、機構側で独自に追加設定が可能であること。
- ④ 収集した全ソフトウェア情報について、ソフトウェアの分類情報、管理対象の区分、ソフトウェアのグルーピングマスターへの登録内容を一覧管理する機能を有すること。
- ⑤ ソフトウェア分類情報を含むソフトウェア辞書の利用に際して、合致しなかった情報の外部機関への提出など、機構の IT 資産情報を外部に出す義務等を負わないこと。
- ⑥ 各種資産台帳への全ての更新業務（例：ライセンス契約情報の登録、インストール情報との関連付け等）について、各管理者 ID 別に、更新日時と更新前内容、更新後内容を、履歴として記録し、把握管理が可能であること。
- ⑦ 基準日等を指定しての不要となった履歴を削除する機能を有すること。

- ⑧ 管理対象 PC の属性情報の各項目について、管理画面から、個別、あるいは複数の管理対象 PC を指定しての一括で、内容を編集更新可能であること。

(6) セキュリティ関連

- ① Microsoft 社セキュリティパッチについて、セキュリティパッチを指定しての適用の有無、未適用のパッチ情報を識別可能であること。
- ② Adobe 社製品 (Adobe Reader, Adobe Flash Player 等) セキュリティパッチ, Java 関連, 各種ブラウザ (Google Chrome, FireFox, Safari) についての、適用されたセキュリティパッチ情報, 未適用のセキュリティパッチ情報を、管理対象 PC 別に把握管理できること。
- ③ ウイルス対策ソフトウェアについては、シマンテック社, トレンドマイクロ社, マカフィー社, ソフォス社, CA 社, ESET 社のコーポレート版の「定義ファイル (パターンファイル) 情報」, 「稼動状態」などの情報を一覧管理できる台帳を作成すること。
- ④ 管理対象 PC に複数のウイルス対策ソフトウェアが導入されている場合、上記③の情報を判定し、当該 PC が安全な状態にあるか否かを識別できる一覧レポート機能を有すること。
- ⑤ これらメーカー以外のウイルス対策ソフトウェアを含めて、ウイルス対策ソフトウェアが未インストールのものを識別可能であること。
- ⑥ 主要なファイル共有ソフトウェア (Winny, Share, BitTorrent, LimeWire, WinMX など) について、管理対象 PC 上の存在を把握可能であること。

Ⅲ. 導入実施と納品に備えるべき要求要件

6. 導入支援作業

6.1. SaaS 型 IT 資産管理システムの利用準備

- ① 機構が所有する管理対象 PC 全 30,000 台が利用する IT 資産管理システムを利用可能な状態とする準備を行うこと。
- ② 管理単位の設定及び利用者 ID の発行に際しては、機構と十分な協議を行い、高精度で負担の少ない管理業務を継続的に行っていくための設定方法等について、他の大学や教育機関の事例等を提供し、円滑に進めること。

6.2. 管理対象 PC へのインストール

- ① 全管理対象 PC への本システムのインストールについて、管理サーバーにログインしてダウンロード実行することで、利用者自身が簡単な方法で実施できるように準備すること。
- ② 管理対象 PC へのインストール時に発生した不具合事象に対しては、メール及び電話にて対応が可能なヘルプデスクを設置すること。ヘルプデスクへの連絡担当者に制限がある場合は機構と協議の上決定すること。
- ③ 管理対象 PC へのインストールの進捗状況は、リアルタイムで各管理者が把握できること。

7. 性能、機能以外に関する要件

7.1. 提案事業者を求める事項

- ① 提案するシステムについては、要求する機能が製品化されていること。
- ② 複数大学における各 5,000 台以上の導入実績を有し、その実績を踏まえ、機構でソフトウェア資産管理を効果的に運用できるよう、適切な助言・支援を行うこと。

7.2. 受注要件

一般財団法人日本情報経済社会推進協会からプライバシーマーク制度によるプライバシーマーク使用許諾、又は、一般財団法人日本情報経済社会推進協会又は海外の認定機関により認定された審査登録機関による情報セキュリティマネジメントシステム(ISMS)の ISO/IEC27001 の認証を受けていること。

7.3. 保守要件

- ① 本調達に、契約期間中におけるソフトウェア保守（サポート）費用を含めること。
- ② 本稼働開始以降の保守・運用支援のため、専門知識を有する要員を確保し、遠隔保守または現地対応の体制を保持すること。
- ③ トラブル対応は迅速かつ確かなものであり、導入ベンダーが直接対応できること。
- ④ メール、電話、FAX での対応に加え、重大なトラブル時などはオンサイトでの対応が可能であること。
- ⑤ 保守対応時間は以下のとおりとする。
「月曜日～金曜日（祝祭日と年末年始 12/29～1/3 を除く） 9 時～ 17 時」対応

(問い合わせ窓口含む) で応答時間が翌営業日以内

- ⑥ 保守にかかる問い合わせ先を機構へ明示すること。また、その保守開始時にメーカー等へのユーザ登録等が必要な場合は、受注者側で登録作業を行うこと。
- ⑦ 保守にかかる問い合わせ内容、問い合わせ者、対応結果（対応途中の時はその見通し）等については取りまとめて翌月 7 日までに月次報告書として機構に提出すること。提出方法や様式の詳細については機構から指示を受けること。
- ⑧ 必要に応じクラウド提供ベンダーと密な連絡を取り業務に当たるものとする。
- ⑨ 本システムのバージョンアップ版が保守契約期間内に限り無償で受けられること。
- ⑩ 本システム内にセキュリティ上の脆弱性等があった場合は、すみやかに機構にその旨連絡し、日程調整の上、対策を講じること。なおシステムの停止が伴わない場合は応札者の判断で対策を最優先とすることができる。
- ⑪ ソフトウェアの障害対応パッチのうち、安定に動作するために必要なもの及びセキュリティ保持に必要なものは、速やかに導入すること。その他、緊急度の低いパッチの導入については、必要に応じて随時導入すること。
- ⑫ ソフトウェア辞書情報など、最新の情報を保守契約期間内で提供されること。

7.4. 操作教育・研修

- ① 各管理者向けマニュアルを作成し、各管理者に対し操作研修を行うこと。日程については本部と協議の上行うこと。
- ② 利用者向けマニュアルおよび利用者向けインストール簡易マニュアルを作成し、各利用担当者に対し操作説明会を行うこと。日程については本部と協議の上行うこと。
- ③ 作成したマニュアルは、編集可能な形式で機構へ提供し、著作権（著作権法第 27 条及び第 28 条の権利を含む）を譲渡すること。（提供マニュアルの内、外部公開しているマニュアル（公式マニュアル）はその限りではない）

7.5. 機密保持

- ① 受注により知り得た全ての情報について守秘義務を負うものとし、これを第三者に漏らし、又は他の目的に使用しないこと。
- ② 受注により知り得た情報については、契約期間はもとより、契約終了後においても第三者に漏らしてはならない。
- ③ 正当な理由があってもやむを得ず第三者に開示する場合、書面によって事前に承諾を得ること。また、情報の厳重な管理を実施すること。
- ④ 機構本部が提供した資料は、原則として全て複製禁止とすること。但し、業務上やむを得ず複製する場合であって、事前に書面にて機構本部の許可を得た場合はこの限りではない。なお、この場合にあっても使用終了後はその複製を機構本部に返納又は焼却・消去する等適切な措置をとり、機密を保持すること。

7.6. 検査及び検収

機構本部担当職員の立ち会いのもと行われる現場での動作確認及び納品成果物（下記）の納入をもって検収とする。

- ① システムの仕様書
- ② システムの操作マニュアル（各管理者向け、利用者向け）
- ③ 利用者向けインストール簡易マニュアル
- ④ システムの設定内容の記述書（ID 情報一覧を含む）

- ⑤ システム試験報告書
- ⑥ 以上全ての文書の電子データ（CD-ROM 格納）

7.7. 損害賠償

受注者が本契約に違反して、機構本部が損害を被った場合には、機構本部は受注者に対して損害賠償を請求し、かつ、機構本部が適当と考える必要な措置をとることを請求できる権利を有するものとする。

7.8. その他

- ① 納入する物品は、中古品であってはならない。
- ② 納入するアプリケーションソフト、システムについて、バージョンアップ、製造中止が発生した場合、技術的要件及び価格が同等である場合は、最新版を導入すること。
- ③ 本調達の履行について疑義が生じたとき、又は本調達に伴い機構本部と交わす契約書に定めない事項については、機構本部及び受注者の双方で協議の上決定すること。
- ④ 受注者の故意又は過失により損害が発生した場合は、受注者の責により現状復帰すること。
- ⑤ 本調達物品を導入するに当たっては、当機構から「国立高専機構情報セキュリティポリシー」に基づき、情報セキュリティに係る事項等の説明を受け遵守すること。
- ⑥ 本調達を導入事例としてパンフレット発行等の各種メディアへの掲載やプレス発表を行う場合は、必ず機構と調整の上とり行うこと。

以 上